

This redlined draft, generated by CompareRite (TM) - The Instant Redliner, shows the differences between -
original document : Q:\DOCUMENTS\YEAR 2000\P001996-HOFFMANNSECRET
COMMUNICATION KEY\ORIGINAL SPECIFICATION.DOC
5 and revised document: Q:\DOCUMENTS\YEAR 2000\P001996-
HOFFMANNSECRET COMMUNICATION KEY\SUBSTITUTE
SPECIFICATION.DOC

CompareRite found 172 change(s) in the text

Deletions appear as Overstrike text surrounded by []
Additions appear as Bold-Underline text

SPECIFICATION

TITLE

METHOD AND ARRANGEMENT FOR FORMING A SECRET COMMUNICATION
KEY FOR A PREDETERMINED ASYMMETRIC CRYPTOGRAPHIC KEY PAIR

BACKGROUND OF THE INVENTION

Field of the Invention

1 The invention relates to a method and an arrangement for forming a secret communication key for a predetermined asymmetric key pair.

Description of the Related Art

2 The formation of an asymmetric cryptographic key pair is known from C.

25 Ruland, Informationssicherheit in Datennetzen, ISBN 3-89238-081-3,
DATACOM-Verlag, page 79 - 85, 1993 (Ruland I), which discloses[[1].

~~Given this method,~~ the RSA method for forming a cryptographic key pair, which comprises a secret (**private**) key and a corresponding public key~~[, is formed]~~. Only
30 the user knows the ~~[secret]~~ **private** key~~[, but]~~ the public key can be made known to all subscribers of a communication network. **In this method, the** ~~[The]~~ user signs the data with his ~~[secret]~~ **private** key when a digital signature is prepared for protecting the authenticity and integrity of electronic data. The signed digital signature is verified upon utilization of the public key corresponding to the ~~[secret]~~
35 **private** key, so that the authenticity or~~[, respectively,]~~ integrity of the digital signature can be checked by all communication partners, ~~[which]~~ **who** have access to the public key. The ~~[aforementioned what is referred to as a]~~ **Public Key**

Technology@] previously mentioned "Public-Key-Technology" is particularly applied in the digital communication within a computer network (a fixed number of computer units, which are connected to one another via a communication network). Given the method known from ~~[[1]]~~ **Ruland**, the protection of the ~~[secret]~~ **private** key against unauthorized access of a third party is of critical importance for the security of the digital signature.

3 It is known from ~~[[2]]~~ **D. Longley and M. Shain, Data & Computer Security, Dictionary of standards concepts and terms, Stockton Press, ISBN 0-333-42935-4, page 317, 1987 (Longley)** to store the ~~[secret]~~ **private** key on an external medium for storing data, for example, a chip card, a disk etc., or on a hard disk, ~~[whereby]~~ **where** key data are protected in that a personal identification code (Personal Identification Number, PIN) or a password, with which the key data **that** are respectively deciphered is used. It is necessary, however, to access the local resources of a user when these external media are used. This is not desired especially with respect to a network-oriented infrastructure of network computers or Java applications. **These are defined as follows.** A network computer is a computer~~[, which]~~ **that** is networked with other computers; **and a**~~[~~

A] Java application is a program containing programs that are written in the programming language Java. **The** ~~[Therefore, the]~~ method known from ~~[[2]]~~ is ~~associated with the disadvantage]~~ **Longley is disadvantageous in** that the ~~[secret]~~ **private** key must be stored on an external medium, so that it is very difficult to protect the ~~[secret]~~ **private** key against misuse.

4 An overview regarding hash functions can be found in ~~[[3]]~~ **C. Ruland, Informationssicherheit in Datennetzen, ISBN 3-89238-081-3, DATACOM-Verlag, page 68 - 73, 1993 (Ruland II)**. A hash function is a function~~[, wherein]~~ **in which** it is possible to calculate a corresponding input value to a given function value. Furthermore, an output character string having a fixed length is allocated to an arbitrarily long input character string. Moreover, additional properties can be requested for the hash function~~[. Such an additional property is]~~, **such as** collision freedom, ~~[i.e., it is not allowed to be possible to find]~~ **which precludes the possibility of finding** two different input character strings resulting in the same output character string. Examples of a hash function are the method according to

the MD-2 standard, the method according to the MD-5 standard, the Data Encryption Standard (DES), which is carried out without utilizing a key, or any other arbitrary hash function.

5 5 A method referred to as a [method according to Miller-Rabin, wherein it can
be checked for] **"Miller-Rabin" can determine whether** a number [whether it] is [a]
prime [number,] **or not. Such a method** is known from [[4-]] **A. J. Menezes, P. van
Oorschot and S. Vanstone, Handbook of Applied Cryptography, CRC Press,
ISBN 0-8493-8523-7, page 138 - 140, 1997 (Menezes).**

10 ~~[Therefore, an]~~ **SUMMARY OF THE INVENTION**

6 An object of the invention is to form a secret communication key for a predetermined asymmetric cryptographic key pair, ~~wherein~~ **where** the ~~secret~~ **private** key of the asymmetric key pair must not be stored permanently.

7 The problem is solved by ~~the method and by the arrangement with the~~
15 ~~features of the independent patent claims.~~

a method for forming a secret communication key for a predetermined asymmetric cryptographic key pair which comprises a private key and a corresponding public key, by a computer, comprising the steps of utilizing a prescribable initial value given a determination of the key pair; providing the initial value to a user; entering, by the user, the initial value into the computer; and forming the secret communication key upon utilization of the initial value, the secret communication key and the public key forming an asymmetric cryptographic communication key pair.

25 **8 The problem is also solved by an arrangement comprising an input device configured for entering an initial value by a user; and a processor connected to the input device, the processor configured to implement the above method.**

9 Given the method for forming a secret communication key for a predetermined
30 asymmetric cryptographic key pair, which comprises a ~~[secret]~~ private key and a
corresponding public key, a prescribable initial value ~~[has been]~~(that is available to
a user) is used with respect to the determination of the key pair. ~~[The initial value is~~
~~available to a user.]~~ The user enters the initial value into the computer and the secret

communication key is formed upon utilization of the initial value. The secret communication key and the public key form a communication key pair, **which is not to be confused with the predetermined asymmetric cryptographic key pair.**

10

5

} The arrangement for forming a secret communication key for a predetermined asymmetric cryptographic key pair, which comprises a ~~{secret}~~ **private** key and a corresponding public key, has a processor, which is set up such that the following steps can be carried out:

- 10 - a prescribed initial value ~~{has been}~~ **is** used for determining the key pair,
 - the user enters the initial value into the computer,
 - the secret communication key is formed upon utilization of the initial value,
~~{whereby}~~ **where** the secret communication key and the public key form a communication key pair.

15 **11** Furthermore, an input ~~{means}~~ **device** is provided for entering the initial value by the user.

12 As a result of the invention, it is possible to erase the ~~{secret}~~ **private** key without having to forego the intense cryptography of the ~~{APublic-Key-Technology@}~~ **"Public-Key-Technology"**.

20 Concretely, the initial value can be regarded as a personal identification code (Personal Identification Number_ PIN) or as a password that is prescribed by the user or that is centrally prescribed and that is entered by the user into the computer. After the password or ~~{, respectively,}~~ the PIN has been entered, the secret communication key, i.e., the key that is of the same name compared to the ~~{secret}~~ **private** key, is
25 formed, which forms a ~~{key pair, the}~~ communication key pair ~~{,}~~ together with the public key **(i.e., the communication key pair comprises the public key and the secret communication key)**, upon utilization of the ~~{the {sic}}~~ password or ~~{, respectively,}~~ of the PIN as an initial value.

~~{[sic]}~~

30

13 In this way, a fusion of the password technology customary to the user of a conventional computer network or ~~{, respectively,}~~ of a conventional computer with

the intense cryptology is inventively achieved without considerable efforts being necessary in order to permanently store ~~[secret]~~ private key material.

14 Preferred embodiments of the ~~[invention derive from the dependent claims.~~

5]method and associated apparatus for implementing the method are provided as follows. The inventive method may further comprise the steps of: supplying the initial value to a hash function; and determining, using a hash function value formed by the hash function, the key pair and the communication key pair. The formation of the communication key pair may
10 further include additional data characterizing the user. The method may further comprise the steps of: determining a prime number based on the initial value, where, in an iterative method, the following steps are performed: 1) checking the initial value or a previously checked number, producing a checked number, to determine whether the checked number is a prime number
15 and (determination of primacy), and if the checked number is a prime, storing an index, which refers to a plurality of numbers, which have been checked with respect to their property of being prime; and 2) selecting, when the number is not a prime number, another number based on the checked number and the index, the checked number being increased by a prescribed number; where
20 the method further comprises the steps of: erasing a used prime number after the communication key pair has been formed; and forming, with the index and the initial value, a new communication key pair for forming the secret communication key.

25 **15** The inventive methods and associated apparatus are described in more detail below.

16 In an embodiment of the invention, a hash function is applied to the initial value, ~~[whereby]~~ providing a value ~~[is]~~ being formed that is finally used for the key generation. Furthermore, additional data, which preferably characterize the user himself, can be used during the key generation. The RSA method for the key
30 generation is preferably used for forming the cryptographic key. The method according to the MD-5 standard, the MD-2 standard or the Data Encryption Standard (DES) can be used as a hash function ~~[can be used [sic]]~~. The communication key pair can be used for enciphering or for securing the integrity of electronic data, for

forming a digital signature via electronic data or for authenticating a user~~[-]~~;
generally for any arbitrary cryptographic operation using the ~~[A~~Public-Key-
Technology~~@, whereby]~~ **"Public-Key-Technology" that uses** the formed
communication key pair ~~[is utilized]~~.

5 }.

17 For accelerating the method, it is advantageous in an embodiment to store an
index **(accelerating code)** when the ~~[secrete]~~ **private** key is formed~~[-, which index is~~
~~referred to as accelerating code in the following]~~. The accelerating code indicates
how often numbers - proceeding from the initial value - have been checked to the
10 effect whether or not the respective number is a prime number. The method
according to Miller-Rabin is preferably used for checking the property whether a
number represents a prime number.

BRIEF DESCRIPTION OF THE DRAWINGS

15 **18** An exemplary embodiment of the invention is shown in the Figures and is
subsequently explained in greater detail.

~~{Shown are~~

}Figure 1 **is** a flow diagram representing the method steps of the exemplary
20 embodiment;

Figure 2 ~~[a-drawing]~~ **is a block diagram** representing a computer network
having a plurality of computers coupled to one another; **and**

Figure 3 **is** a symbolic **block** drawing representing the course of action for
determining a prime number on the basis of an initial value.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

19 Figure 2 shows a plurality of computers 200, 210, 220, 230, 240, 250, which
are connected to one another via a communication network 260. Each computer
200, 210, 220, 230, 240, 250 respectively has a plurality of input ~~[means,]~~ **devices**,
30 i.e., a keyboard 206, 216, 226, 236, 246, 256, a mouse 207, 217, 227, 237, 247,
257, a scanner (not shown) or a camera (not shown). The entered information is
supplied to a memory 202, 212, 222, 232, 242, 252 via the respective input ~~[means]~~
device via an input interface/output interface 201, 211, 221, 231, 241, 251 and is

stored. The 202, 2212, 222, 232, 242, 252 memory is connected to the input interface/output interface 201, 211, 221, 231, 241, 251 via a bus 204, 214, 224, 234, 254. A processor 203, 213, 223, 233, 243, 253, which is set up such that the following methods steps can be carried out, is also connected to the bus 204, 214, 224, 234, 254.

20 The computer 200, 210, 220, 230, 240, 250 communicate via the communication network 260 according to the Transport Control Protocol/Internet Protocol (TCP/IP). The communication network 260 also contains a certification unit 270 with which a certificate is prepared respectively for a public key, so that the public key is trustworthy for a communication on the basis of the ~~[A~~Public-Key-Technology@]“Public-Key-Technology”. A user 280 enters an arbitrary prescribable word (PIN, password), which is only known to the user, into a first computer 200 (step 101, compare Figure 1).

21 According to the RSA method, the first computer 200 generates an asymmetric cryptographic key pair, as described in the following. The value 102 entered by the user 280 and additional data 103 characterizing the user 280, such as user name, personal number, terminal address etc., are supplied to a hash function (step 104). ~~The~~[[3] contains an overview regarding hash functions. A] hash function is ~~[a function, wherein it is not possible to calculate a corresponding input value to a given function value. Furthermore, an output character string having a fixed length is allocated to an arbitrarily long input character string. Moreover, additional]~~ **defined and has** properties **as described above** ~~[can be requested for the hash function. Such an additional property is collision freedom, i.e., it is not allowed to be possible to find two different input character strings resulting in the same output character string.~~

~~Examples of a hash function are the method according to the MD-2 standard, the method according to the MD-5 standard, the Data Encryption Standard (DES), which is carried out without utilizing a key, or any other arbitrary hash function].~~ The value formed by the hash function is used as a base value BW for forming two prime numbers, as symbolically shown in Figure 3. As shown in Figure 3, it is respectively checked for a value W_i ($i = 1, \dots, n$) in an iterative method, on the basis of the base

value BW, whether or not the respective value represents a prime number (step 301).

22 The method according to Miller-Rabin is utilized as method for checking the property prime for a number (see Menezes). If the number[[4]].

5

If it is determined ~~[for a number that the number does not represent a prime number]~~
to not be prime, the number is increased by a prescribable value, preferably by the
value 2 (step 302) and the test with respect to the property ~~[A prime@]~~ "prime" is
repeated (step 301). This course of action is repeated until two prime numbers - a
10 first prime number ~~[P]~~ p and a second prime number q - have been determined.

10

~~[Referred]~~ **23 A number, referred** to as an index ~~[is a number indicating]~~, indicates
how often - on the basis of the base value ~~[PW-[sic]]~~ BW- the number must be
increased by the prescribed value until the first prime number p or~~[, respectively,]~~ the
second prime number q is obtained. The result of the method shown in Figure 3 is
15 two prime numbers p and q, which are used for the key generation according to the
RSA method (step 105). The prime numbers p and q normally have a length of a
~~[plurality]~~ multiple of 100 ~~[bit]~~ bits. A modulus n is formed from the prime numbers p
and q according to the following rule:

15

20
$$n = p * q. \quad (1)$$

24 Furthermore, an intermediate variable ~~[n(n)]~~ $\phi(n)$ is formed according to the
following rule:

25
$$\phi(n) = (p-1) * (q-1). \quad (2)$$

25 A secret key d is now selected such that the secret key d is relatively prime
with respect to $\phi(n)$. A public key e is determined such that the following rule is
fulfilled:

30

$$e * d \mod \phi(n) = 1. \quad (3)$$

26 The value d is the ~~{secret}~~ **private** key and is not allowed to ~~{make}~~ **be made** known to a third party. **A** ~~[Therefore, a]~~ private key d (step 106) and a public key e (step 107) have been formed as a result of the key generation (key 105). The two keys d, e form a cryptographic key pair corresponding to one another, this key pair
5 being used for an arbitrary cryptographic operation, i.e., for enciphering, deciphering, for ~~{the}~~ **a** digital signature, or for authenticating (step 108).

27 After the key pair d, e has been formed according to the above-described method, the ~~{secret}~~ **private** key d is erased. The public key e is supplied to the certification entity 280. A certificate Certe is formed by the certification entity 280 via
10 the public key e and the certificate Certe of the public key e is stored in a directory 290 that can be accessed by the public. Therefore, each communication participant in the communication network 280 can access the public key e via the certificate Certe of the public key e. The secret key d corresponding to the public key e is erased in the first computer 200.

28 Every time ~~{when}~~ **that** the user 280 wishes to initial a communication on the basis of the key pair or~~[, respectively,]~~ when the user 280 wishes to carry out a cryptographic operation upon utilization of such a key pair, the user ~~{208-~~{sic}~~}~~ **280** enters his initial value (PIN, password) into the first computer 200 and the initial value 102 (as described above), in turn, is provided with additional data 103~~[,].~~ **It is**
15 **then** subjected to a hash function (step 104) and, on the basis of the base value BW, two prime numbers p and q are determined or a stored index (as described above) is read out or is also entered by the user 280 and a ~~{secrete}~~ **secret** communication key is formed ~~{therefrom}~~ **from it**, which, however, corresponds to the ~~{secrete,}~~ **private** previously formed key d, which has been erased again.

29 In this way, a communication key pair has been formed, which comprises the ~~{secrete}~~ **secret** communication key and the corresponding public key e. For a communication session, a user can thus respectively ~~{currently}~~ **immediately** generate the ~~{secrete}~~ **secret** communication code, so that it is possible to use
25 intense ~~{A Public-Key-Technology@}~~ **"Public-Key-Technology"** without having to store the ~~{secrete}~~ **secret** key on a chip card. The ~~{thus}~~ generated communication key pair d, e is used for enciphering plaintext 109 with the public key e and for deciphering the electronic, enciphered data 110 with the ~~{secrete}~~ **secret** communication key.
30

30 Figure 1 symbolically shows the processing of plaintext 109, i.e., electronic data 109 that can be read by everybody, as well as enciphered electronic data 110, ~~[whereby]~~ **where** the communication device **is** respectively ~~[describes]~~ **described** by an arrow toward or~~[-, respectively,]~~ from the block representing a cryptographic operation 108.

~~[[sic]~~

31 The enciphering or, respectively, deciphering is performed according to the following rules:

$$m^e \bmod n = c, \quad (4)$$

~~[whereby]~~ **where**

- m refers to a quantity of 512 bit of electronic data 109 to be enciphered,
- c refers to enciphered electronic data 110.

32 The deciphering of the enciphered electronic data c is performed according to the following rule:

$$m = c^d \bmod n. \quad (5)$$

33 A few alternatives of the above-described exemplary embodiment are explained **as follows**. ~~[in the following:]~~

} The method can be used for enciphering, for securing integrity and for ~~[the]~~ **a** digital signature of electronic data. Furthermore, the invention can be utilized in the field of secure electronic mail systems. The user must not necessarily enter the initial value 102 during the generation of the key pair at the beginning of the method, but a central unit generating the key pair can prescribe it to the user. Therefore, the user must merely remember a password or~~[-, respectively,]~~ a PIN₁ and it is no longer necessary to securely store a ~~[secrete]~~ **secret** cryptographic key, for example₁ on a chip card, ~~[this being]~~ **which is** associated with corresponding risks and with

considerable outlay. Instead of a hash function, any arbitrary one-way function can be used in the framework of the invention.

~~[The following publications have been cited in the framework of this document.]~~ **34**

5 **The above-described method and arrangement are illustrative of the principles of the present invention. Numerous modifications and adaptations will be readily apparent to those skilled in this art without departing from the spirit and scope of the present invention.**

~~[[1] C. Ruland, Informationssicherheit in Datennetzen,]~~ **ABSTRACT**

~~[ISBN 3-89238-081-3, DATACOM-Verlag, page 79 – 85, 1993~~

5 ~~[2] D. Longley and M. Shain, Data & Computer Security,
Dictionary of standards concepts and terms, Stockton Press,
ISBN 0-333-42935-4, page 317, 1987~~

~~[3] [1] C. Ruland, Informationssicherheit in Datennetzen,
10 ISBN 3-89238-081-3, DATACOM-Verlag, page 68 – 73, 1993~~

~~[4] A. J. Menezes, P. van Oorschot and S. Vanstone, Handbook of Applied
Cryptography, CRC Press, ISBN 0-8493-8523-7, page 138 – 140, 1997
Abstract~~

15

~~Method and arrangement for forming a **secrete** communication key for a
predetermined asymmetric cryptographic key pair~~

~~[35 After a key pair with a public key and a corresponding **[secrete]** **private** key
20 has been determined on the basis of an initial value, the initial value is made
available to a user. The **[secrete]** **private** key can **then** be erased. When the user
wishes to carry out a cryptographic operation based on the **[APublic-Key-
Technology@]**“**Public-Key-Technology**”, the user enters the initial value into a
computer and, upon utilization of the initial value, a **[secrete]** **secret** communication
25 key is formed, which corresponds to the **[secrete]** **private** key **that had been**
previously formed but **was then** erased **[since-]**.
[Sign. Figure 1]~~

Appendix A
Mark Ups for Claim Amendments

This redlined draft, generated by CompareRite (TM) - The Instant Redliner, shows the differences between -
original document : Q:\DOCUMENTS\YEAR 2000\P001996-HOFFMANNSECRET
COMMUNICATION KEY\ORIGINAL CLAIMS.DOC
and revised document: Q:\DOCUMENTS\YEAR 2000\P001996-
HOFFMANNSECRET COMMUNICATION KEY\AMENDED CLAIMS.DOC

CompareRite found 154 change(s) in the text

Deletions appear as Overstrike text surrounded by []
Additions appear as Bold-Underline text

1. ~~[Method]~~**(Amended) A method** for forming a ~~[secrete]~~ **secret** communication key for a predetermined asymmetric cryptographic key pair~~[-]~~ which comprises a ~~[secrete]~~ **private** key and a corresponding public key, by a computer, **comprising the steps of:**

utilizing ~~[a)-whereby]~~ a prescribable initial value ~~[has been used]~~ given ~~[the]~~ **a** determination of ~~[the]~~ **said** key pair~~[-]~~;

~~[b)-whereby the]~~ **providing said** initial value ~~[is made available]~~ to a user~~[-]~~;

~~[c)-whereby the user enters the]~~ **entering, by said user, said** initial value into ~~[the]~~ **said** computer; **and**~~[-]~~

~~[d)-whereby the secrete]~~ **forming said secret** communication key ~~[is formed]~~ upon utilization of ~~[the]~~ **said** initial value, ~~[whereby the secrete]~~ **said secret** communication key and ~~[the]~~ **said** public key ~~[form]~~ **forming** an asymmetric cryptographic communication key pair.

2. ~~[Method]~~**(Amended) The method** according to claim 1, **further comprising the steps of:**

supplying said ~~[whereby the]~~ initial value ~~[is supplied]~~ to a hash function ~~[and the]; and~~

determining, using a hash function value formed by ~~{the}~~ said hash function ~~{is used for determining the}~~, said key pair and ~~{the}~~ said communication key pair.

5 3. ~~{Method}~~**(Amended) The method** according to claim 1 ~~{or 2,}~~ **further comprising the step of:**
 ~~{whereby}~~ **including** additional data characterizing ~~{the}~~ said user ~~{are utilized}~~ when ~~{the}~~ said key pair and ~~{the}~~ said communication key pair are formed.

10 4. ~~{Method}~~**(Amended) The method** according to ~~{one of the claims 1 to 3,}~~ **claim 1, further comprising the steps of:**

~~{whereby}~~ **determining** a prime number ~~{is determined on the basis of the}~~ **based on said** initial value, ~~{whereby}~~ **where**, in an iterative method, ~~{it is}~~ **the following steps are performed:**

15 **checking said initial value or a previously checked number, producing a checked number, to determine** whether ~~{the respectively}~~ said checked number is a prime number and ~~{when this is the case,}~~**(determination of primacy), and if said checked number is a prime, storing** an index ~~{is stored}~~, which refers to a plurality of numbers, which have been checked with respect to their
20 property ~~{whether they are}~~ **of being prime; and**

selecting, when said number is not a prime number, ~~{is stored}~~ ~~{sic}~~, ~~otherwise,}~~ another number ~~{is selected on the basis of the}~~ **based on said** checked number and ~~{the index is}~~ **said index, said checked number being** increased by a prescribed number~~{,}~~;

25 ~~{whereby the}~~ **said method further comprising the steps of:**
 erasing a used prime number ~~{is erased}~~ after ~~{the}~~ said communication key pair has been formed; **and**~~{,}~~

~~{whereby the index and the}~~ **forming, with said index and said** initial value ~~{are respectively used for forming}~~, a new communication key pair for forming ~~{the~~ **secret}** said secret communication key.
30

5. ~~[Method]~~**(Amended) The method** according to claim 4, **wherein said determination of primacy for any given number** ~~[whereby the test, whether a number is a prime number,]~~ is carried out according to the method of Miller-Rabin.

5

6. ~~[Method]~~**(Amended) The method** according to **claim 1 wherein** ~~[one of the claims 1 to 5,~~
~~whereby the]~~ keys are formed according to the RSA method.

10

7. ~~[Method]~~**(Amended) The method** according to **claim 2 wherein said** ~~[one of the claims 2 to 6,~~
~~whereby the]~~ hash function is **selected from the group consisting of the methods**
~~[one of the following methods:~~
~~-]MD-5 method, the[-] MD-2 method, and[-the method according to]~~ the Data
Encryption Standard (DES) **method** as **a** one-way function.

15

8. ~~[Method]~~**(Amended) The method** according to **claim 1, further comprising the step of:** ~~[one of the claims 1 to 7,~~
~~used for]~~

20

enciphering electronic data with ~~[the secret]~~ **said secret** communication key.

9. ~~[Method]~~**(Amended) The method** according to **claim 1, further comprising the step of:** ~~[one of the claims 1 to 7,~~
~~used for]~~

25

forming a digital signature via electronic data ~~[upon utilization of the secret]~~
using said secret communication key.

10. ~~[Method]~~**(Amended) The method** according to **claim 1, further comprising the step of:** ~~[one of the claims 1 to 7,~~
~~used for]~~

30

authenticating ~~[upon utilization of the secret]~~ data using said secret
communication key.

11. ~~[Arrangement]~~ **(Amended) An arrangement** for forming a ~~[secret]~~
5 secret communication key for a predetermined asymmetric cryptographic key pair[,]
which comprises a ~~[secret]~~ private key and a corresponding public key, ~~[with a~~
comprising:

an input device configured for entering an initial value by a user; and
a processor ~~[being set up such that the following steps can be carried out:~~
10 connected to said input device, said processor configured to:

~~[the key pair has been determined upon utilization of a]~~ determine,
using said prescribable initial value, said asymmetric cryptographic key pair;
accept entry of said ~~[the]~~ initial value ~~[is]~~ made available to ~~[a user,~~
said user; and

15 ~~[the user enters the initial value into the computer,~~
~~the secret]~~ form said secret communication key ~~[is formed upon utilization of the]~~
using said initial value, ~~[whereby the secret]~~ where said secret communication
key and ~~[the]~~ said public key form a communication key pair~~[, and]~~.

20 ~~[with an input means for entering the initial value by the user.~~

12. ~~Arrangement]~~ **12. (Amended) The arrangement** according to claim 11,
wherein said ~~[whereby the]~~ processor is ~~[set up]~~ configured such that ~~[the]~~ said
initial value is supplied to a hash function and ~~[the]~~ a hash value formed by the hash
25 function is used for determining ~~[the]~~ said asymmetric cryptographic key pair and
the communication key pair.

13. ~~[Arrangement]~~ **(Amended) The arrangement** according to claim 11,
wherein said ~~[or 12,~~

whereby the processor is ~~set up~~ **configured** such that additional data characterizing ~~the~~ **said** user are utilized during ~~the~~ **said** formation of ~~the~~ **said asymmetric cryptographic** key pair and ~~the~~ **said** communication key pair.

5 14. ~~[Arrangement]~~**(Amended) The arrangement** according to **claim 11**, **wherein said** ~~one of the claims 11 to 13,~~

whereby the processor is ~~set up such that~~ **configured to:**

~~[determine]~~ a prime number ~~[is determined on the basis of the]~~ **based on** **said** initial value, ~~[whereby]~~ **where**, in an iterative method~~[, it]~~:

10 **said initial value or a previously checked number** is checked, **producing a checked number, to determine** whether ~~the~~ **said** checked number is a prime number ~~[and when this is the case,]~~**(determination of primacy)**, and **if said checked number is a prime, storing** an index ~~[is stored]~~, which refers to a plurality of numbers, which have been checked with respect to their
15 property ~~[whether they are]~~ **of being prime; and**

select, when said number is not a prime number, ~~[is stored [sic],~~
~~otherwise,]~~ another number ~~[is selected on the basis of the]~~ **based on said** checked number and ~~the index is]~~ **said index, said checked number being** increased by a prescribed number~~[,];~~

20 ~~[whereby the]~~ **said processor further being configured to:**

erase a used prime number ~~[is erased]~~ after ~~the~~ **said** communication key pair has been formed; **and**~~[,]~~

~~[whereby the]~~ **form, with said** index and ~~the~~ **said** initial value ~~[are respectively used for forming]~~, a new communication key pair for forming ~~the~~
25 ~~secrete]~~ **said secret** communication key.

15. ~~[Arrangement]~~**(Amended) The arrangement** according to claim 14, **wherein said** ~~whereby the~~ processor is ~~set up such that the test, whether a number is a prime number, is performed]~~ **configured carry out said determination**
30 **of primacy** according to the method of Miller-Rabin.

16. ~~{Arrangement}~~**(Amended) The arrangement** according to claim 11,
wherein said ~~{one of the claims 11 to 15,~~
whereby the processor is ~~{set up such that the}~~ **configured to form** keys ~~{are~~
5 ~~formed}~~ according to the RSA method.

17. ~~{Arrangement}~~**(Amended) The arrangement** according to claim 12,
wherein said ~~{one of the claims 12 to 16,~~
whereby the processor is ~~{set up such that the}~~ **configured to produce said** hash
10 function ~~{is one of the following methods~~
~~Method}~~ according to **a method selected from the group consisting of the** ~~{one~~
of the claims 2 to 6,
whereby the hash function is one of the following methods:
~~MD-5 method, the~~ MD-2 method, **and** ~~{the method according to}~~ the Data
15 Encryption Standard (DES) **method** as one-way function.

18. ~~{Method}~~**(Amended) The arrangement** according to claim 11 ~~{one of the~~
claims 11 to 17,
} used for enciphering electronic data with ~~{the secret}~~ **said secret** communication
20 key.

19. ~~{Arrangement}~~**(Amended) The arrangement** according to claim 11 ~~{one~~
of the claims 11 to 17,
} used for forming a digital signature via electronic data upon utilization of ~~{the~~
25 ~~secret}~~ **said secret** communication key.

20. ~~{Arrangement}~~**(Amended) The arrangement** according to claim 11 ~~{one~~
of the claims 11 to 17,
} used for authenticating **data** upon utilization of ~~{the secret}~~ **said secret**
30 communication key.